

## AMENDMENTS TO THE CLAIMS

No claims are added.

Claims 3, 6, 8, 12 and 16 are original.

Claims 1, 5, 7, 11, 15 and 17—19 are currently amended.

Claim 4 was previously presented.

Claims 2, 9, 10, 13 and 14 were previously cancelled.

Accordingly, claims 1 and 3—8, 11—12, 15—19 are pending.

1. (Currently Amended) A system for porting user data from one computer to another, comprising:

a memory device configured to store the user data and a public key; and

a smart card associated with a user that alternately enables access to the user data on the memory device when both the memory device and smart card are interfaced with a common computer and disables access to the user data when ~~one of the memory device or smart card is absent; and~~

wherein the public key is sent from the memory device stores a public key and to the smart card, wherein the smart card contains stores a corresponding private key, and wherein access to the user data in the memory device is enabled upon verification that the public key and the private key are associated[[.]] as a public/private key pair such that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key may be decrypted by the private key; and

wherein the smart card is configured to pass an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

1  
2           2.     (Cancelled)

3  
4           3.     (Original) An assembly as recited in claim 1, wherein the smart card  
5 stores a passcode and access to the user data in the memory device is enabled upon  
6 authentication of a user-supplied passcode to the passcode stored on the smart  
7 card.

8  
9           4.     (Previously Presented) An assembly as recited in claim 1, wherein  
10 the memory device stores a user's profile that can be used for computer  
11 configuration.

1           5.       (Currently Amended) A profile carrier comprising:

2           a smart card to store a passcode and a private key from a private/public key  
3 pair; and

4           a memory device to store a user profile and a public key from the  
5 private/public key pair;

6           ~~wherein~~ wherein, when the smart card and the memory device are  
7 interfaced with a common computing unit, the smart card is configured to permit  
8 use of the private key following validation of a user-entered passcode with the  
9 stored passcode and to authenticate, using the private key, the public key ~~stored on~~  
10 sent to the smart card from the memory device using the private key, wherein the  
11 authentication requires that the public and private keys are components of an  
12 asymmetric cryptographic system whereby data encrypted by the public key may  
13 be decrypted by the private key; and

14           wherein the profile carrier ~~is being~~ configured to permit access to the user  
15 profile stored on the memory device upon successful authentication of the public  
16 key at the smart card; and

17           wherein the smart card is configured to pass an encryption key to the  
18 memory device for decryption of data read from the memory device, and for  
19 encryption of data to be stored on the memory device.

20  
21           6.       (Original) A computer system, comprising:

22           a computing unit having a memory drive and a smart card reader; and

23           the profile carrier as recited in claim 5, wherein the memory device is  
24 interfaced with the computing unit via the memory drive and the smart card is  
25 interfaced with the computing unit via the smart card reader.

1  
2 7. (Currently Amended) A computer system, comprising:

3 a computer having an interface; and

4 a profile carrier adapted to use the interface, the profile carrier comprising a  
5 smart card associated with a user, the smart card containing a private key, and a  
6 memory device having data memory to store a user's profile, the memory device  
7 storing a public key associated with the private key, wherein the smart card  
8 alternately enables access to the user's profile when present and disables access to  
9 the user's profile when absent;

10 ~~wherein the smart card contains a first key;~~

11 ~~wherein the data memory contains a second key that is associated with the~~  
12 ~~first key; and~~

13 ~~wherein the smart card is configured to authenticate the second key from~~  
14 ~~the data memory using the first key as a condition for enabling access to the user~~  
15 ~~data.~~

16 wherein the system is configured to send the public key from the memory  
17 device to the smart card, and wherein access to the user data in the memory device  
18 is enabled upon verification that the public key and the private key are associated  
19 as a public/private key pair such that the public and private keys are components  
20 of an asymmetric cryptographic system whereby data encrypted by the public key  
21 may be decrypted by the private key; and

22 wherein the smart card is configured to pass an encryption key to the  
23 memory device for decryption of data read from the memory device, and for  
24 encryption of data to be stored on the memory device.  
25

1           8.     (Original) A computer system as recited in claim 7, wherein the  
2 smart card stores a passcode and is configured to authenticate a user-supplied  
3 passcode entered into the computer as a condition for enabling access to the user  
4 data.

5  
6           9.     (cancelled)

7  
8           10.    (cancelled)

9  
10          11.    (Currently Amended) A computer system, comprising:  
11 a computer having a memory drive and a card reader;  
12 a portable profile carrier to port a user's profile for configuration of the  
13 computer, the profile carrier comprising:

14           (a) an integrated circuit (IC) card associated with the user that can be  
15 interfaced with the computer via the card reader; and

16           (b) a memory device to store the user's profile, the memory device  
17 being interfaced with the computer via the memory drive, the IC card enabling  
18 access to the user data on the memory device;

19           wherein when the profile carrier is interfaced with the computer, the user's  
20 profile is accessible to configure the computer;

21           wherein the IC card stores a passcode and a private key of a public/private  
22 key pair;

23           wherein the memory device stores a public key of the public/private key  
24 pair; and  
25

1 wherein the IC card is configured to authenticate a user-supplied passcode  
2 entered into the computer as a condition for enabling access to the private key and  
3 to authenticate the public key ~~passed in~~ sent from the memory device to the IC  
4 card, using the private key as a condition for enabling access to the user's profile  
5 wherein the authentication requires confirmation that the public and private keys  
6 are components of an asymmetric cryptographic system whereby data encrypted  
7 by the public key may be decrypted by the private key; and

8 wherein the smart card is configured to pass an encryption key to the  
9 memory device for decryption of data read from the memory device, and for  
10 encryption of data to be stored on the memory device.

11  
12 12. (Original) A computer system as recited in claim 11, wherein the IC  
13 card stores a passcode and is configured to authenticate a user-supplied passcode  
14 entered into the computer as a condition for enabling access to the user's profile.

15  
16 13. (Cancelled)

17  
18 14. (Cancelled)

1           15. (Currently Amended) A method for porting a user profile for a  
2 computer, comprising:

3           storing a user profile in memory of a smart card secured profile carrier, the  
4 smart card secured profile carrier having a smart card that selectively enables  
5 access to the user profile in the memory;

6           interfacing the smart card secured profile carrier with the computer; and

7           sending a public key, stored in the memory, to the smart card;

8           verifying that a private key, stored on the smart card, is associated with the  
9 public key, received from the memory, as a public/private key pair, wherein the  
10 association requires that the public and private keys are components of an  
11 asymmetric cryptographic system whereby data encrypted by the public key may  
12 be decrypted by the private key, and wherein the public key is stored within the  
13 memory and sent to the smart card to facilitate the verifying;

14           reading the user profile from the memory, upon a successful verification,  
15 for use in configuring the computer; and

16           ~~wherein the memory device stores a public key and the smart card stores a~~  
17 ~~corresponding private key and access to the user data in the memory device is~~  
18 ~~enabled upon verification that the public key and the private key are associated.~~

19           passing an encryption key, from the smart card and to the memory device,  
20 for decryption of data read from the memory device, and for encryption of data to  
21 be stored on the memory device.

1  
2 16. (Original) A method as recited in claim 15, further comprising  
3 interfacing the smart card secured profile carrier with a different second computer  
4 and reading the user profile from the memory for use in configuring the second  
5 computer.

6  
7 17. (Currently Amended) A method comprising:  
8 storing user data and a public key on a portable memory device;  
9 storing a private key on a smart card;  
10 interfacing the smart card and the portable memory device with a computer;  
11 sending the public key to the smart card;  
12 verifying compatibility of the public key and the private key, wherein the  
13 verification requires that the public and private keys are components of an  
14 asymmetric cryptographic system whereby data encrypted by the public key may  
15 be decrypted by the private key; and  
16 passing an encryption key, from the smart card and to the memory device,  
17 for decryption of data read from the memory device, and for encryption of data to  
18 be stored on the memory device; and  
19 allowing, in response to the verified compatibility, access to the user data  
20 on the portable memory device.  
21  
22  
23  
24  
25

1           18.   (Currently Amended) A method comprising:  
2           storing user data in a portable memory device;  
3           storing a ~~device-resident-public~~ key in the memory device;  
4           storing a ~~eard-resident-private~~ key on the smart card, the card-resident key  
5           corresponding to the device-resident key;  
6           storing a passcode on the smart card;  
7           interfacing the smart card with a computer;  
8           interfacing the portable memory device with the computer;  
9           receiving a user-entered passcode;  
10          permitting use of the ~~eard-resident-private~~ key following validation of the  
11          user-entered passcode with the passcode stored on the smart card;  
12          passing the ~~device-resident-public~~ key from the memory device to the smart  
13          card;  
14          authenticating, at the smart card, the ~~device-resident-public~~ key using the  
15          ~~eard-resident-private~~ key, thereby confirming that the public key and the private  
16          key are associated as a public/private key pair, such that the public and private  
17          keys are components of an asymmetric cryptographic system whereby data  
18          encrypted by the public key may be decrypted by the private key; and  
19          permitting access to the user data stored in the memory device upon  
20          successful authentication of the ~~device-resident-public~~ key[.]; and  
21          passing an encryption key, from the smart card and to the memory device,  
22          for decryption of data read from the memory device, and for encryption of data to  
23          be stored on the memory device.  
24  
25

1 19. (Currently Amended) In a system having a computer and a smart card  
2 secured profile carrier, the smart card secured profile carrier having memory to  
3 store a user profile and a smart card separate from the memory, computer-readable  
4 media resident on the profile carrier having executable instructions comprising:

5 receiving a user-supplied passcode from the computer;

6 authenticating the user-supplied passcode with a passcode stored on the  
7 smart card;

8 enabling access to a private key on the smart card upon successful  
9 authentication of the user-supplied passcode;

10 ~~receiving~~ sending a public key from the memory to the smart card;

11 authenticating the public key using the private key, thereby confirming that  
12 the public key and the private key are a public/private key pair, such that the  
13 public and private keys are components of an asymmetric cryptographic system  
14 whereby data encrypted by the public key may be decrypted by the private key;  
15 and

16 enabling access to the user profile in the memory upon successful  
17 authentication of the public key. key; and

18 passing an encryption key, from the smart card and to the memory device,  
19 for decryption of data read from the memory device, and for encryption of data to  
20 be stored on the memory device.  
21  
22  
23  
24  
25